AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) A method ~~Method~~ for ensuring the integrity of at least one computer software program which can be carried out by means of at least one encryption/decryption module, the at least one computer software program being transmitted, by means of a transmitter, to a decoder which is equipped with the at least one encryption/decryption module by means of a long-distance information transmission network, the transmitter performing the steps comprising:

~~the transmitter carrying out:~~

a) a step (40) for encrypting information signals transmitted to the decoder,

b) a step (50) for transmitting, to the at least one encryption/decryption module of the decoder, a message containing the information required for the decoder to decrypt the information signals transmitted at step a), and

c) a step (42, 100) for transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder,

the decoder carrying out:

d) a step (74) for decrypting the information signals transmitted by the transmitter during step a) using the information provided for this purpose in the message transmitted during step b),

e) a step for constructing a single identifier for a group of several computer software programs to be transmitted during step c) based on information relating to each of the software programs of the group and in that the at least one encryption/decryption module carries out the same operation as that carried out during step e) in order to reconstruct a unique identifier corresponding to that constructed during step e) if the group received by the decoder is identical to that transmitted by the transmitter,

~~characterised:~~wherein,

~~— in that —~~the transmitter inserts (at 52, 124) in the message transmitted during step b) an additional item of information which allows the at least one encryption/decryption module to verify that it has effectively received the or each computer software program transmitted at step c),

~~— in that —~~the at least one encryption/decryption module verifies (at 60), based on the additional information inserted by the transmitter in the message transmitted during step b), whether it has effectively received the or each software program transmitted during step c), and

~~, in that,~~ if the or each software program has not been received, the at least one encryption/decryption module prevents step d) (at 68).

2. (currently amended) The method ~~Method~~ according to claim 1, ~~characterised in that~~ wherein the transmitter encrypts (at 50) the message transmitted at step b), and in that the at least one encryption/decryption module decrypts the message transmitted during step b) in order to allow step d) to be carried out.

3. (currently amended) The method ~~Method~~ according to claim 1, ~~characterised in that~~ wherein the transmitter carries out:

~~e) a step (44, 122) for constructing a first identifier of the or each computer software program transmitted during step c), and~~

f) a step (52, 124) for inserting this identifier in the message transmitted during step b),

and in that the at least one encryption/decryption module carries out:

g) a step (62, 110) for reconstructing the identifier of the or each computer software program based on the or each computer software program received,

h) a step (66, 112) for comparing the identifier reconstructed at step g) with the identifier inserted by the transmitter during step f), and

i) if the identifier reconstructed at step g) does not correspond to that inserted at step f) in the message transmitted at step b), a step (68, 108) for preventing step d),

j) if the identifier reconstructed at step g) corresponds to the identifier inserted at step f) in the message transmitted during step b), a step (66, 112) for validating the integrity of the or each computer software program.

4. (cancelled)

5. (currently amended) The method ~~Method~~ according to claim 3, ~~characterised in that~~wherein the steps d), g), h), i) and j) are carried out by the same encryption/decryption module.

6. (currently amended) The method ~~Method~~ according to claim 3, ~~characterised in that~~ wherein a first autonomous encryption/decryption module carries out only steps d), h), i) and j), and in that a second autonomous encryption/decryption module which is independent from the first encryption/decryption module and which is fixedly joined to the decoder carries out at least step g).

7. (currently amended) The method ~~Method~~ according to claim 6, ~~characterised in that~~ wherein the transmitter further ~~carries out~~ performing the steps comprising:

k) a second step (120) for constructing a second identifier of the or each computer software program transmitted during step c), this second identifier being transmitted together with the or each corresponding software program during step c), and

- in that step g) which is carried out by the second encryption/decryption module comprises:

- an operation (102) for reconstructing the second identifier which is transmitted together with the or each software program,

- only if the second reconstructed identifier corresponds to that transmitted together with the or each software program during step c), an operation (110) for reconstructing the first identifier inserted in the message transmitted during step b) and for transmitting this first reconstructed identifier to the first encryption/decryption module so that the first encryption/decryption module can carry out step h).

8. (currently amended) The method ~~Method~~ according to claim 7, ~~characterised in that~~ wherein the first and the second identifiers are obtained from the same identifier of the or each computer software program by encrypting the same identifier using a different first and second encryption key, respectively.

9. (currently amended) The method ~~Method~~ according to claim 2, ~~characterised in that~~ wherein the at least one encryption/decryption module carries out the at least one computer software program each time the integrity thereof is validated during step j).

10. (currently amended) An information ~~Information~~ recording medium (12) with a computer program recorded thereon comprising instructions for carrying out a method according to claim 1, when the instructions are carried out by the transmitter (4).

11. (currently amended) An information ~~Information~~ recording medium (22, 88) with a computer program recorded thereon comprising instructions for carrying out a method according to claim 1, when the instructions are to be carried out by the at least one encryption/decryption module.

12. (currently amended) A system ~~System~~ for ensuring the integrity of at least one computer software program which can be carried out by at least one encryption/decryption module (16, 84), the system comprising:

a transmitter (4) for transmitting the at least one computer software program via a long-distance information transmission network (8), and a decoder (6, 82) which is equipped with the at least one encryption/decryption module (16, 84),

the transmitter (4) being capable of:

- encrypting information signals transmitted to the or each decoder,

- transmitting to the at least one encryption/decryption module of the decoder a message containing the information required for the decoder to decrypt the information signals transmitted, and

- transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder,

- the decoder (6, 82) being capable of decrypting the information signals transmitted by the transmitter using the information which is provided for this purpose and which is contained in the message transmitted by the transmitter,

- constructing a single identifier for a group of several computer software programs to be transmitted during the transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder based on information relating to each of the software programs of the group and in that the at least one encryption/decryption module carries out the same operation as that carried out during constucting in order to reconstruct a unique identifier corresponding to that constructed during constucting if the group received by the decoder is identical to that transmitted by the transmitter,

~~characterised:~~wherein,

~~- in that~~ the transmitter (4) is capable of inserting in the message an additional item of information which allows the at least one encryption/decryption module (46, 84) to verify that it has received the or each computer software program transmitted,

~~- in that~~ the at least one encryption/decryption module (16, 84) is capable of verifying, based on the additional information inserted by the transmitter in the message, whether it has effectively received the or each software program transmitted by the transmitter, and

~~— in that,~~ if the or each software program has not been received, the at least one encryption/decryption module (16, 84) is capable of preventing the decryption of the information signals transmitted.

13. (currently amended) The system ~~System~~ according to claim 12, ~~characterised in that~~ wherein the or each decoder (6) is equipped with a single removable encryption/decryption module.

14. (currently amended) The system ~~System~~ according to claim 12, ~~characterised in that~~ wherein the or each decoder (82) is equipped with at least two autonomous encryption/decryption modules which are independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder.

15. (currently amended) A transmitter ~~Transmitter~~ (4) which is suitable for carrying out a method according to claim 1, this transmitter (4) being capable of:

- encrypting information signals transmitted to the or each decoder,

- transmitting to the at least one encryption/decryption module of the decoder a message containing the information required for the decoder to decrypt the information signals transmitted, and

- transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder,

~~characterised:~~wherein

~~— in that —~~the transmitter (4) is capable of inserting in the message an additional item of information which allows the at least one encryption/decryption module (46, 84) to verify that it has received the or each computer software program transmitted.

16. (currently amended) The decoder ~~Decoder —~~(6, 82) which is suitable for carrying out a method according to claim 1, this decoder (6, 82) being capable of decrypting the information signals transmitted by the transmitter using the information which is provided for this purpose and which is contained in the message transmitted by the transmitter, and being equipped with the at least one encryption/decryption module (16, 84);

~~characterised:~~wherein,

~~— in that —~~the at least one encryption/decryption module (16, 84) is capable of verifying, based on the additional information inserted by the transmitter in the message, whether it has effectively received the or each software program transmitted by the transmitter, and

~~— in that,~~ if the or each software program has not been received, the at least one encryption/decryption module (16, 84) is capable of preventing the decryption of the information signals transmitted.

17. (currently amended) The decoder ~~Decoder —~~(6, 82) according to claim 16, ~~characterised in that~~wherein the decoder ~~it —~~is equipped with a single removable encryption/decryption module.

18. (currently amended) The decoder ~~Decoder —~~(6, 82) according to claim 16, ~~characterised in that~~ wherein the decoder ~~it —~~is equipped with at least two autonomous encryption/decryption modules which are independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder.

19. (currently amended) The method ~~Method —~~according to claim 2, ~~characterised in that —~~the transmitter carries out:

~~c) a step (44, 122) for constructing a first identifier of the or each computer software program transmitted during step c), and~~

f) a step (52, 124) for inserting this identifier in the message transmitted during step b),

and in that the at least one encryption/decryption module carries out:

g) a step (62, 110) for reconstructing the identifier of the or each computer software program based on the or each computer software program received,

h) a step (66, 112) for comparing the identifier reconstructed at step g) with the identifier inserted by the transmitter during step f), and

i) if the identifier reconstructed at step g) does not correspond to that inserted at step f) in the message transmitted at step b), a step (68, 108) for preventing step d),

j) if the identifier reconstructed at step g) corresponds to the identifier inserted at step f) in the message transmitted during step b), a step (66, 112) for validating the integrity of the or each computer software program.

20.(currently amended) Method according to claim ~~4~~ 1, ~~characterised in that~~ wherein a first autonomous encryption/decryption module carries out only steps d), h), i) and j), and in that a second autonomous encryption/decryption module which is independent from the first encryption/decryption module and which is fixedly joined to the decoder carries out at least step g).